

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-224461

(43)Date of publication of application : 17.08.1999

(51)Int.CI.

G11B 20/10
G09C 1/00
H04L 9/32

(21)Application number : 10-025310

(71)Applicant : SONY CORP

(22)Date of filing : 06.02.1998

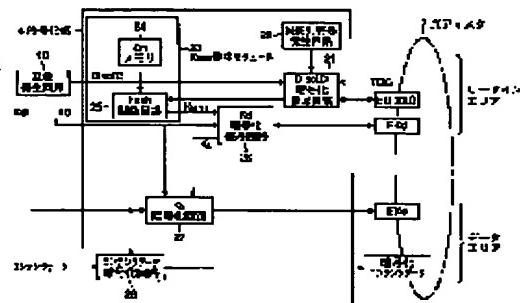
(72)Inventor : ASANO TOMOYUKI
OSAWA YOSHITOMO
HASHIMOTO MEGUMI

(54) INFORMATION PROCESSOR, INFORMATION METHOD, PROVIDING MEDIUM AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain intrinsic information in a recording medium by decoding the intrinsic information in the recording medium which are read out from the medium and are ciphered with an M series code.

SOLUTION: At first, a disk ID encryption decoding circuit 21 receives an EDiscID which is read out from the read-in area of an optical disk 7 and which is an ciphered DiscID. Next, the circuit 21 generates an EDiscID by decoding the EDiscID based on the predetermined M series code which is supplied from an M series code generating circuit 22 to output it to the hash function circuit 25 of an effective master key generating module 23. Moreover, M series codes to be supplied from the circuit 22 are codes which are given when proper licences are granted from copyright holders.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-224461

(43) 公開日 平成11年(1999)8月17日

(51) Int.Cl.⁶
G 1 1 B 20/10
G 0 9 C 1/00
H 0 4 L 9/32

識別記号

F I		
G 1 1 B	20/10	H
G 0 9 C	1/00	6 6 0 D
H 0 4 L	9/00	6 7 3 E

審査請求 未請求 請求項の数9 OL (全 11 頁)

(21)出願番号 特願平10-25310

(22)出願日 平成10年(1998)2月6日

(71)出願人 000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号

(72)発明者 浅野 智之
東京都品川区北品川6丁目7番35号 ソニー
一株式会社内

(72)発明者 大澤 義知
東京都品川区北品川6丁目7番35号 ソニー
一株式会社内

(72)発明者 橋本 恵
東京都品川区北品川6丁目7番35号 ソニー
一株式会社内

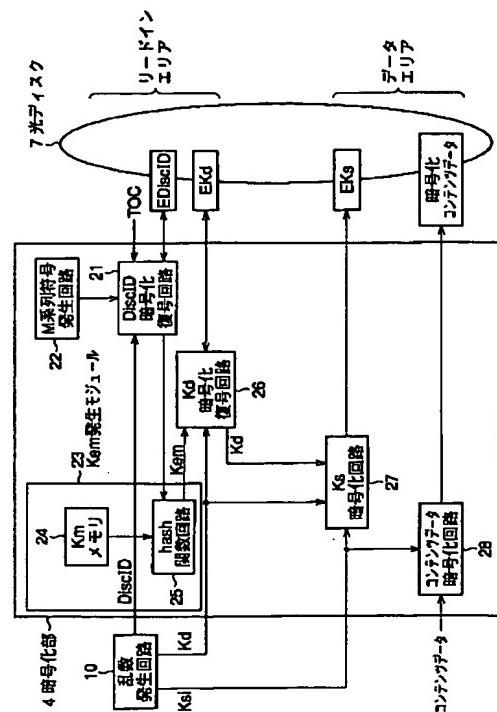
(74)代理人 弁理士 稲本 義雄

(54) 【発明の名称】 情報処理装置、情報処理方法、提供媒体、および記録媒体

(57) 【要約】

【課題】 記録媒体から読み出された暗号化された記録媒体の固有情報をM系列符号で復号し、記録媒体の固有情報を得る。

【解決手段】ステップS31において、DiscID暗号化復号回路21は、光ディスク7のリードインエリアから読み出された、暗号化されたDiscIDであるEDiscIDを受け取る。DiscID暗号化復号回路21はさらに、ステップS32において、M系列符号発生回路22から供給された予め定められたM系列符号に基づいて、EDiscIDを復号して、DiscIDを生成し、Kem発生モジュール23のhash関数回路25に出力する。M系列符号回路22が供給するM系列符号は、著作権者から適正なライセンスを受けるときに、与えられたものである。



【特許請求の範囲】

【請求項 1】 着脱可能な記録媒体に情報を記録または再生する情報処理装置において、

第1の秘密キーを発生する発生手段と、

前記記録媒体からそこに記録されている暗号化された前記記録媒体の固有情報を受信する受信手段と、

前記発生手段により発生された第1の秘密キーにより、前記受信手段により受信した暗号化された前記記録媒体の固有情報を復号し、前記記録媒体の固有情報を生成する生成手段とを備えることを特徴とする情報処理装置。

【請求項 2】 前記記録媒体から暗号化された前記記録媒体の固有情報を受信できないとき、乱数を発生する乱数発生手段と、

前記第1の秘密キーにより、前記乱数を前記記録媒体の固有情報として暗号化し、前記記録媒体に記録する記録手段とをさらに備えることを特徴とする請求項1に記載の情報処理装置。

【請求項 3】 前記生成手段により生成された前記記録媒体の固有情報と、第2の秘密キーに基づいて、第3の秘密キーを算出する算出手段と、

前記算出手段により算出された前記第3の秘密キーに対応して、所定の情報を暗号化し、前記記録媒体に記録する記録手段とをさらに備えることを特徴とする請求項1に記載の情報処理装置。

【請求項 4】 前記所定の情報は、前記記録媒体に固有の秘密キーであることを特徴とする請求項3に記載の情報処理装置。

【請求項 5】 前記第3の秘密キーにより、前記記録媒体から再生された前記記録媒体に固有の暗号化されている第4の秘密キーを復号する復号手段をさらに備え、前記記録手段に、復号された前記第4の秘密キーを利用して、所定の情報を暗号化し、前記記録媒体に記録することを特徴とする請求項3に記載の情報処理装置。

【請求項 6】 前記第3の秘密キーにより、前記記録媒体から再生された前記記録媒体に固有の暗号化されている第4の秘密キーを復号する第1の復号手段と、復号された前記第4の秘密キーを利用して、前記記録媒体から供給された暗号化されているデータを復号する第2の復号手段とをさらに備えることを特徴とする請求項3に記載の情報処理装置。

【請求項 7】 着脱可能な記録媒体に情報を記録または再生する情報処理装置の情報処理方法において、

第1の秘密キーを発生する発生ステップと、

前記記録媒体からそこに記録されている暗号化された前記記録媒体の固有情報を受信する受信ステップと、

前記発生ステップにより発生された第1の秘密キーにより、前記受信ステップにより受信した暗号化された前記記録媒体の固有情報を復号し、前記記録媒体の固有情報を生成する生成ステップとを備えることを特徴とする情報処理方法。

【請求項 8】 着脱可能な記録媒体に情報を記録または再生する情報処理装置に使用するコンピュータプログラムであって、

第1の秘密キーを発生する発生ステップと、

前記記録媒体からそこに記録されている暗号化された前記記録媒体の固有情報を受信する受信ステップと、

前記発生ステップにより発生された第1の秘密キーにより、前記受信ステップにより受信した暗号化された前記記録媒体の固有情報を復号し、前記記録媒体の固有情報を生成する生成ステップとを備えるコンピュータプログラムを提供することを特徴とする提供媒体。

【請求項 9】 情報処理装置に装着され、情報が記録または再生される記録媒体において、

M系列符号で暗号化した前記記録媒体に固有の情報が記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、情報処理装置、情報処理方法、提供媒体、および記録媒体に関し、特に、より安全にデータを授受することを可能にする情報処理装置、情報処理方法、提供媒体、および記録媒体に関するもの。

【0002】

【従来の技術】 近年、情報をデジタル的に記録する記録機器および記録媒体が普及しつつある。これらの記録機器および記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データを、その質を維持しながら何度もコピーすることができる。しかしながら、映像や音楽のデータの著作権者にしてみれば、自らが著作権を有するデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまう恐れがある。このため、記録機器および記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ必要がある。

【0003】 例えば、ミニディスク（MD）（商標）システムにおいては、SCMS（Serial CopyManagement System）と呼ばれる方法が用いられている。これは、デジタルインターフェースによって、音楽データとともに伝送される情報のことである。この情報は、音楽データが、copy free、copy once allowed、またはcopy prohibitedのうちのいずれのデータであるのかを表す。ミニディスクレコーダーは、デジタルインターフェースから音楽データを受信した場合、SCMSを検出し、これが、copy prohibitedであれば、音楽データをミニディスクに記録せず、copy once allowedであれば、これをcopy prohibitedに変更し、受信した音楽データとともに記録し、copy freeであれば、これをそのまま、受信した音楽データとともに記録する。

【0004】 このようにして、ミニディスクシステムにおいては、SCMSを用いて、著作権を有するデータが不正

にコピーされるのを防いでいる。

【0005】また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、Digital Versatile Disk(DVD)（商標）システムにおける、コンテンツスクリンブルシステムがあげられる。このシステムでは、ディスク上の、著作権を有するデータが全て暗号化され、ライセンスを受けた記録機器だけが暗号鍵を与えられ、これにより暗号化されたデータを復号し、意味のあるデータを得ることができるようになされている。そして、記録機器は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、DVDシステムにおいては、著作権を有するデータが不正にコピーされるのを防いでいる。

【0006】

【発明が解決しようとする課題】しかしながら、上記のミニディスクシステムが採用している方式では、SCMSがcopy once allowedであれば、これをcopy prohibitedに変更し、受信したデータとともに記録するなどの動作規定に従わない記録機器が、不正に製造されてしまう。

【0007】また、上記のDVDシステムが採用している方式は、ROMメディアに対しては有効であるが、ユーザがデータを記録可能なRAMメディアにおいては有効ではない。RAMメディアにおいては、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録機器で動作するディスクを新たに作ることができるからである。

【0008】本発明はこのような状況に鑑みてなされたものであり、例えば、著作権者から適正に利用許可を受けた者にだけ与えられる秘密キーに基づいて、記録媒体に固有の情報にアクセスできるようにすることで、不正コピーを防止するものである。

【0009】

【課題を解決するための手段】請求項1に記載の情報処理装置は、第1の秘密キーを発生する発生手段と、記録媒体からそこに記録されている暗号化された記録媒体の固有情報を受信する受信手段と、発生手段により発生された第1の秘密キーにより、受信手段により受信した暗号化された記録媒体の固有情報を復号し、記録媒体の固有情報を生成する生成手段とを備えることを特徴とする。

【0010】請求項7に記載の情報処理方法は、第1の秘密キーを発生する発生ステップと、記録媒体からそこに記録されている暗号化された記録媒体の固有情報を受信する受信ステップと、発生ステップにより発生された第1の秘密キーにより、受信ステップにより受信した暗号化された記録媒体の固有情報を復号し、記録媒体の固有情報を生成する生成ステップとを備えることを特徴とする情報処理方法。

【0011】

請求項8に記載の提供媒体は、第1の秘密

キーを発生する発生ステップと、記録媒体からそこに記録されている暗号化された記録媒体の固有情報を受信する受信ステップと、発生ステップにより発生された第1の秘密キーにより、受信ステップにより受信した暗号化された記録媒体の固有情報を復号し、記録媒体の固有情報を生成する生成ステップとを備えるコンピュータプログラムを提供することを特徴とする。

【0012】請求項9に記載の記録媒体は、M系列符号で暗号化した記録媒体に固有の情報が記録されていることを特徴とする。

【0013】請求項1に記載の情報処理装置、請求項7に記載の情報処理方法、および請求項8に記載の提供媒体においては、第1の秘密キーが発生され、記録媒体からそこに記録されている暗号化された記録媒体の固有情報を受信され、発生された第1の秘密キーにより、受信した暗号化された記録媒体の固有情報を復号され、記録媒体の固有情報を生成される。

【0014】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を附加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0015】請求項1に記載の情報処理装置は、第1の秘密キー（予め定められたM系列符号）を発生する発生手段（例えば、図3のM系列符号発生回路22）と、記録媒体からそこに記録されている暗号化された記録媒体の固有情報（EDiscID）を受信する受信手段（例えば、図3のDiscID暗号化復号回路21）と、発生手段により発生された第1の秘密キーにより、受信手段により受信した暗号化された記録媒体の固有情報を復号し、記録媒体の固有情報（DiscID）を生成する生成手段（例えば、図3のDiscID暗号化復号回路21）とを備えることを特徴とする。

【0016】請求項2に記載の情報処理装置は、記録媒体から暗号化された記録媒体の固有情報を受信できないとき、乱数を発生する乱数発生手段（例えば、図3の乱数発生回路10）と、第1の秘密キーにより、乱数を記録媒体の固有情報として暗号化し、記録媒体に記録する記録手段（例えば、図3のDiscID暗号化復号回路21）とをさらに備えることを特徴とする。

【0017】請求項3に記載の情報処理装置は、生成手段により生成された記録媒体の固有情報と、第2の秘密キー（マスタキーKm）に基づいて、第3の秘密キー（イフェクティブマスタキーKem）を算出する算出手段（例えば、図3のhash関数回路25）と、算出手段により算出された第3の秘密キーに対応して、所定の情報を暗号化し、記録媒体に記録する記録手段（例えば、図3のKd

暗号化復号回路26)とをさらに備えることを特徴とする。

【0018】請求項5に記載の情報処理装置は、第3の秘密キーにより、記録媒体から再生された記録媒体に固有の暗号化されている第4の秘密キー(暗号化ディスクキーEKd)を復号する復号手段(例えば、図3のKd暗号化復号回路26)をさらに備え、記録手段に、復号された第4の秘密キー(マスタキーKd)を利用して、所定の情報を暗号化し、記録媒体に記録することを特徴とする。

【0019】請求項6に記載の情報処理装置は、第3の秘密キーにより、記録媒体から再生された記録媒体に固有の暗号化されている第4の秘密キーを復号する第1の復号手段(例えば、図4のEKd復号回路56)と、復号された第4の秘密キーを利用して、記録媒体から供給された暗号化されているデータを復号する第2の復号手段(例えば、図4のEKs暗号化回路57およびコンテンツデータ復号回路58)とをさらに備えることを特徴とする。

【0020】図1は、本発明を適用した光ディスク記録再生装置の構成例を表している。入力部1は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作されたとき、その入力操作に対応する信号を出力する。制御回路2は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。

【0021】記録再生回路3は、暗号化部4と復号部5を有し、復号部5は、ピックアップ6により、光ディスク7から再生されたデータを復号し、外部に再生信号として出力する。暗号化部4は、外部から記録信号の供給を受け取ると、これを暗号化し、ピックアップ6に供給して、光ディスク7に記録させる。

【0022】ピックアップ6は、レーザビームを光ディスク7に照射することで、データの記録再生を行う。ス

イフェクティブマスタキーKm=hash (マスタキーKm+DiscID) (1)

ここでマスタキーKmは、著作権者等から適正にライセンスを受けた者(光ディスク記録再生装置)にだけ与えられる秘密のキーである。また、ここで、例えば、AとBの結合とは、それぞれが32ビットであるとき、Aの後方にBを結合して、64ビットのデータとすることを意味する。

【0027】光ディスク7のデータエリアの各セクタ S_i ($i=1, 2, \dots$)は、ヘッダおよびメインデータ部で構成され、ヘッダには、セクタキー K_{Si} をディスクキー K_d で暗号化した暗号化セクタキー EK_{Si} ($i=1, 2, \dots$)が格納されている(ここで K_{Si} のiは、セクタの番号を示し、セクタキーはセクタ毎に異なるので K_{Si} と記述するが、特に区別する必要がない場合は、 K_s とも記述する)。メインデータ部には、コンテンツデータをセクタキー K_{Si} で暗号化した暗号化コンテンツデータが格納されている。

スピンドルモータ9は、サーボ回路8によって制御され、光ディスク7を回転させる。

【0023】サーボ回路8は、スピンドルモータ9を駆動することにより、光ディスク7を所定の速度で(例えば線速度一定で)回転させる。サーボ回路8はまた、ピックアップ6のトラッキングおよびフォーカシングの他、スレッドサーボを制御する。乱数発生回路10は、制御回路2の制御により、所定の乱数を発生する。

【0024】光ディスク7には、図2に示すような構造を有するデータが記録されている。光ディスク7のリードインエリアには、光ディスクのID(以下、DiscIDと称する)を予め定められたM系列符号で暗号化したEDiscID、ディスクキー K_d をイフェクティブマスタキー K_m で暗号化した暗号化ディスクキー EK_d が記録されている。

【0025】M系列符号は、所定の周期で、"0"と"1"の2値がランダムに出現する疑似ランダム2値信号(一種の疑似乱数)であり、DiscIDは、例えば、ファイル名やデイレクトリ情報などのTOC(Table Of Contents)データ内に、予め設定された所定のM系列符号に基づいて埋め込むことで暗号化されている。すなわち、DiscIDは、TOCデータのエッジの時間ずれとして記録される。このような暗号化を行うと、TOCデータはM系列符号がなくとも読み取ることができるが(TOCデータは暗号化されないが)、DiscIDはM系列符号がないと読み取る(復号する)ことができなくなる。このようなM系列符号に基づく暗号化に関する技術は、特願平09-288960号として本出願人が先に提案している。なお、この所定のM系列符号は、著作権者から適正なライセンスを受ける際、後述するマスタキー K_m とともに、ライセンスを受けた者に与えられる。

【0026】イフェクティブマスタキー K_m は、式(1)に従い、マスタキー K_m とDiscIDの結合にhash関数を適用して計算される。

【0028】図3は、暗号化部4の構成例を表している。DiscID暗号化復号回路21は、光ディスク7から読み出されたEDiscIDを、M系列符号発生回路22から供給されるM系列符号に基づいて復号し、DiscIDを生成する。DiscID暗号化復号回路21はまた、乱数発生回路10から発生された乱数をDiscIDとして受け取り、M系列符号発生回路22から供給されるM系列符号に基づいて、上述したように、入力されるTOC情報に埋め込むよう暗号化して、EDiscIDを生成し、光ディスク7に記録する。

【0029】M系列符号発生回路22は、例えば、直列接続された複数のフリップフロップとイクスクルーシブオア回路からなり、所定のM系列符号を発生するようになされている。あるいは、ROM、EEPROMなどで構成することもできる。

【0030】Kem発生モジュール23のKmメモリ24は、マスタキーKmを記憶する。Kem発生モジュール23のhash関数回路25は、マスタキーKmとDiscIDの結合を生成し、これにhash関数を適用してイフェクティブマスターKemを算出する。

【0031】Kd暗号化復号回路26は、光ディスク7から読み出された暗号化ディスクキーEKdを、イフェクティブマスターKemで復号して、ディスクキーKdを生成する。Kd暗号化復号回路26はまた、乱数発生回路10から発生された乱数をディスクキーKdとして受け取り、イフェクティブマスターKemで暗号化して暗号化ディスクキーEKdを生成し、光ディスク7に記録する。

【0032】Ks暗号化回路27は、乱数発生回路10から発生された乱数をセクタキーKsとして受け取り、ディスクキーKdで暗号化して暗号化セクタキーEKsを生成し、光ディスク7に記録する。コンテンツデータ暗号化回路28は、セクタキーKsで、コンテンツデータを暗号化し、光ディスク7に記録する。

【0033】次に、図4に、復号部5の構成例を示す。EDiscID復号回路51は、光ディスク7から読み出されたEDiscIDを、M系列符号発生回路52から供給されるM系列符号に基づいて復号して、DiscIDを生成する。M系列符号発生回路52は、M系列符号回路22と同様の構成を有し、M系列符号発生回路22と同一のM系列符号を発生するようになされている。

【0034】Kem発生モジュール53のKmメモリ54は、マスタキーKmを記憶する。Kem発生モジュール53のhash関数回路55は、マスタキーKmとDiscIDの結合を生成し、これにhash関数を適用してイフェクティブマスターKemを計算する。このKem発生モジュール53は、Kem発生モジュール23と同一の構成とされ、両者を兼用するようにしてもよい。

【0035】EKd復号回路56は、光ディスク7から読み出された暗号化ディスクキーEKdを、イフェクティブマスターKemで復号して、ディスクキーKdを算出する。EKs復号回路57は、光ディスク7から各セクタSiのヘッダに記録されている暗号化セクタキーEKsを読み出し、ディスクキーKdで復号して、セクタキーKsを算出する。コンテンツデータ復号回路58は、光ディスク7から読み出された暗号化されたコンテンツデータを、セクタキーKsで復号する。

【0036】次に、ユーザデータが光ディスク7に記録される場合の暗号化部4における処理手順を、図5のフローチャートを参照して説明する。なお、この例の場合、DiscIDは、光ディスク7製造時に、光ディスク7に書き込まれているものとする。

【0037】最初に、ステップS31において、DiscID暗号化復号回路21は、光ディスク7のリードインエリアから読み出された、暗号化されているDiscIDであるEDiscIDを受け取る。DiscID暗号化復号回路21はさら

に、ステップS32において、M系列符号発生回路22から供給された所定のM系列符号に基づいて、EDiscIDを復号して、DiscIDを生成し、Kem発生モジュール23のhash関数回路25に出力する。M系列符号回路22が供給するM系列符号は、著作権者から適正なライセンスを受けるときに、与えられたものである。

【0038】ステップS33において、Kem発生モジュール23のhash関数回路25は、Kem発生モジュール23のKmメモリ24から、マスタキーKmを読み出す。Kem発生モジュール23のhash関数回路25はさらに、ステップS34で、上述の式(1)に従い、光ディスク7のDiscIDとマスタキーKmの結合にhash関数を適用して、イフェクティブマスターKemを計算し、Kd暗号化復号回路26に供給する。

【0039】次に、ステップS35において、Kd暗号化復号回路26は、光ディスク7のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。Kd暗号化復号回路26は、ステップS36で、光ディスク7のリードインエリアに、暗号化ディスクキーEKdが書き込まれているか否か(暗号化ディスクキーEKdを受け取ることができたか否か)の判定を行う。暗号化ディスクキーEKdが書き込まれていないと判定された場合、ステップS37に進み、乱数発生回路10は、40ビットの乱数を発生し、ディスクキーKdとして、Kd暗号化復号回路26に出力する。

【0040】次に、ステップS38において、Kd暗号化復号回路26は、乱数発生回路10から供給されたディスクキーKdを、hash関数回路25から受け取ったイフェクティブマスターKemにより暗号化して、暗号化ディスクキーEKdを生成し、光ディスク7のリードインエリアに記録する。

【0041】ステップS36で、暗号化ディスクキーEKdが書き込まれていると判定された場合、ステップS39に進み、Kd暗号化復号回路26は、この光ディスク7から読み出された暗号化ディスクキーEKdを、hash関数回路25から受け取ったイフェクティブマスターKemで復号して、ディスクキーKdを得る。Kd暗号化復号回路26は、そのディスクキーKdを、Ks暗号化回路27に出力する。

【0042】ステップS38またはS39の処理の後、乱数発生回路10は、ステップS40で、40ビットの乱数を発生し、セクタキーKsとして、Ks暗号化回路27、およびコンテンツデータ暗号化回路28に出力する。Ks暗号化回路27は、ステップS41で、Kd暗号化復号回路26(暗号化ディスクキーEKdが光ディスク7に記録されている場合)、または乱数発生回路10(暗号化ディスクキーEKdが光ディスク7に記録されていない場合)から受け取ったディスクキーKdで、乱数発生回路10から受け取ったセクタキーKsを暗号化して、暗号化セクタキーEKsを生成する。Ks暗号化回路27はま

た、その暗号化セクタキーEKsを、光ディスク7のデータエリアにあるセクタヘッダに記録する。

【0043】次に、ステップS42において、コンテンツデータ暗号化回路28は、(ステップS40で乱数発生回路10から受け取った)セクタキーKsにより、コンテンツデータを暗号化し、光ディスク7のデータエリアのメインデータ部に記録する。

【0044】ステップS43において、暗号化部4の各回路は、全てのコンテンツデータを記録したか否かの判定を行う。全てのコンテンツデータがまだ記録されていないと判定された場合、ステップ44に進み、暗号化部4の各回路は、光ディスク7の、まだデータを記録していないセクタにアクセスし、ステップS40に戻り、以下同様の処理を繰り返す。ステップS43で、全てのコンテンツデータが記録されたと判定された場合、暗号化部4の各回路は、全ての記録処理を終了する。

【0045】以上のようにして、著作権者から適正なライセンスを受けるときに、与えられた所定のM系列符号で、暗号化されたDiscIDを復号し、DiscIDを得ることにより、暗号化した情報が記録媒体に記録される。

【0046】次に、製造時に、DiscIDが記録されていない光ディスク7に対して、ユーザデータを記録する場合の暗号化部4における処理手順を、図6のフローチャートを参照して説明する。

【0047】最初に、ステップS51において、DiscID暗号化復号回路21は、光ディスク7のリードインエリアから読み出されたEDiscIDを受け取り、またKd暗号化復号回路26は、光ディスク7のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。

【0048】次に、ステップS52において、DiscID暗号化復号回路21は、光ディスク7のリードインエリアに、EDiscIDが書き込まれているか否か(EDiscIDを受けることができたか否か)の判定を行い、Kd暗号化復号回路26は、光ディスク7のリードインエリアに、暗号化ディスクキーEKdが書き込まれているか否か(暗号化ディスクキーEKdを受け取ることができたか否か)の判定を行う。EDiscIDと暗号化ディスクキーEKdが共に書き込まれないと判定された場合、ステップS53に進み、乱数発生回路10は、128ビットの乱数を発生し、DiscIDとして、DiscID暗号化復号回路21に出力する。

【0049】次に、ステップS54において、DiscID暗号化復号回路21は、乱数発生回路10から供給されたDiscIDを、M系列符号発生回路22から供給されたM系列符号に基づいて、上述したように、TOC情報中に埋め込むようにして暗号化して、EDiscIDを生成し、光ディスク7のリードインエリアに記録する。

【0050】次に、ステップS55において、Kem発生モジュール23のhash関数回路25は、Kem発生モジュール23のKmメモリ24から、マスタキーKmを読み出

す。Kem発生モジュール23のhash関数回路25は、ステップS56で、上述の式(1)に従い、光ディスク7のDiscID、およびKmメモリ24から読み出したマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、Kd暗号化復号回路26に供給する。

【0051】次に、ステップS57において、乱数発生回路10は、40ビットの乱数を発生し、ディスクキーKdとして、Kd暗号化復号回路26に出力する。Kd暗号化復号回路26は、ステップS58において、乱数発生回路10から供給されたディスクキーKdを、hash関数回路25から受け取ったイフェクティブマスタキーKemにより暗号化して、暗号化ディスクキーEKdを生成し、光ディスク7のリードインエリアに記録する。

【0052】ステップS52で、EDiscIDと暗号化ディスクキーEKdが書き込まれていると判定された場合、ステップS59に進み、DiscID暗号化復号回路21は、この光ディスクから読み出されたEDiscIDを、M系列符号回路22から供給されたM系列符号で復号して、DiscIDを生成する。

【0053】ステップS60において、Kem発生モジュール23のhash関数回路25は、Kem発生モジュール23のKmメモリ24から、マスタキーKmを読み出す。Kem発生モジュール23のhash関数回路25は、ステップS61で、上述の式(1)に従い、光ディスク7のDiscIDとマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、Kd暗号化復号回路26に供給する。

【0054】次に、ステップS62において、Kd暗号化復号回路26は、この光ディスク7から読み出された暗号化ディスクキーEKdを、hash関数回路25から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを得る。Kd暗号化復号回路26は、ディスクキーKdを、Ks暗号化回路27に出力する。

【0055】ステップS58またはS62の処理の後は、ステップS63に進むが、ステップS63乃至S67で行われる処理は、図5のステップS40乃至S44で行われる処理と同様の処理であり、全てのコンテンツデータが記録されたと判定された場合、全ての記録処理が終了する。

【0056】以上のようにして、DiscIDが生成され、記録媒体に記録され、そして生成されたDiscIDとマスタキーKmに対応して暗号化されたコンテンツデータが記録媒体に記録される。このことより、例えば、既存の記録媒体(DiscIDが記録されていない記録媒体)に複製されたコンテンツデータを、著作権者から適正にライセンスを受けていない者は、意味のある情報として再生することができない。

【0057】次に、図7のフローチャートを参照して、復号部5により行われる、ユーザデータの再生処理を説

明する。最初に、ステップS 8 1において、EDiscID復号回路5 1は、光ディスク7のリードインエリアから読み出された、暗号化されたDiscIDであるEDiscIDを受け取る。EDiscID復号回路5 1はさらに、ステップS 8 2において、M系列符号発生回路5 2から供給されたM系列符号に基づいて、EDiscIDを復号してDiscIDを生成し、Kem発生モジュール5 3のhash関数回路5 5に出力する。

【0058】次に、ステップS 8 3において、Kem発生モジュール5 3のhash関数回路5 5は、EDiscID復号回路5 1から出力されたDiscIDを受け取るとともに、Kmメモリ5 4からマスタキーKmを読み出し、上述の式(1)に従い、光ディスク7のDiscIDとマスタキーKmの結合にhash関数を適用してイフェクティブマスタキーKemを算出し、EKd復号回路5 6に供給する。

【0059】ステップS 8 4において、EKd復号回路5 6は、光ディスク7のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。EKd復号回路5 6は、ステップS 8 5で、この読み出された暗号化ディスクキーEKdを、hash関数回路5 5から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを算出し、EKs復号回路5 7に出力する。

【0060】次に、ステップS 8 6において、EKs復号回路5 7は、光ディスク7のデータエリアから読み出された各セクタの暗号化セクタキーEKsi ($i=1, 2, \dots$) を受け取る。EKs復号回路5 7は、ステップS 8 7で、この読み出された暗号化セクタキーEKsiを、EKd復号回路5 6から受け取ったディスクキーKdで復号して、セクタキーKsiを算出し、コンテンツデータ復号回路5 8に出力する。

【0061】ステップS 8 8において、コンテンツデータ復号回路5 8は、光ディスク7から読み出された暗号化されているコンテンツデータを受け取る。コンテンツデータ復号回路5 8は、ステップS 8 9で、この読み出された暗号化されているコンテンツデータを、EKs復号回路5 7から受け取ったセクタキーKsiで復号し、再生信号として出力する。

【0062】次に、ステップS 9 0において、復号部5の各回路は、光ディスク7のデータエリアから、全てのコンテンツデータを読み出したか否かの判定を行う。全てのコンテンツデータがまだ読み出されていないと判定された場合、ステップS 9 1に進み、復号部5の各回路は、光ディスク7の、まだ読み出されていない次のセクタのデータの供給を受け、ステップS 8 6以降の処理を繰り返す。全てのコンテンツデータが読み出されたと判定された場合、復号部5の各回路は、全ての再生処理を終了する。

【0063】このように、記録媒体のIDを生成し、所定のM系列符号で暗号化して、記録媒体に記録することで、著作権者から適正にライセンスを受けた者だけが、

その記録媒体にアクセスできるようにする。

【0064】本発明は、光ディスク以外の記録媒体にデータを記録または再生する場合にも適用が可能である。

【0065】なお、本明細書中において、上記処理を実行するコンピュータプログラムをユーザに提供する提供媒体には、磁気ディスク、CD-ROMなどの情報記録媒体の他、インターネット、デジタル衛星などのネットワークによる伝送媒体も含まれる。

【0066】

【発明の効果】請求項1に記載の情報処理装置、請求項7に記載の情報処理方法、および請求項8に記載の提供媒体によれば、第1の秘密キーにより、記録媒体に記録されている暗号化された記録媒体の固有情報を復号し、記録媒体の固有情報を生成するようにしたので、例えば、予め定められたM系列符号を有していない者が、記録媒体にアクセスすることを困難にする。

【0067】請求項2に記載の情報処理装置によれば、記録媒体から暗号化された記録媒体の固有情報を受信できないとき、乱数を記録媒体の固有情報として暗号化し、記録媒体に記録するようにしたので、例えば、予め定められたM系列符号を有していない者は、記録媒体の固有情報が記録されていない記録媒体に記録されている情報を、再生することができない。

【0068】請求項3に記載の情報処理装置によれば、生成手段により生成された記録媒体の固有情報と、第2の秘密キーに基づいて、第3の秘密キーを算出し、算出された第3の秘密キーに対応して、所定の情報を暗号化し、記録媒体に記録するようにしたので、予め定められたM系列符号を有していない者が、記録媒体にアクセスすることを、さらに困難にする。

【0069】請求項9に記載の記録媒体によれば、M系列符号で暗号化した記録媒体に固有の情報を記録するようにしたので、情報処理装置に記録媒体の固有情報を提供することができる。

【図面の簡単な説明】

【図1】本発明を適用した光ディスク記録再生装置の一実施の形態の構成を示すブロック図である。

【図2】光ディスクに記録されるデータを説明する図である。

【図3】図1の暗号化部4の内部の構成を示す図である。

【図4】図1の復号部5の内部の構成を示す図である。

【図5】図1の暗号化部4の動作を説明するフローチャートである。

【図6】図1の暗号化部4の他の動作を説明するフローチャートである。

【図7】図1の復号部5の動作を説明するフローチャートである。

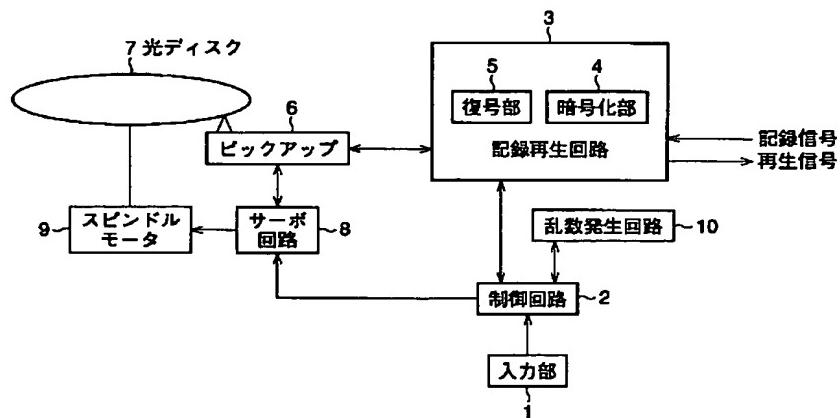
【符号の説明】

1 入力部, 2 制御回路, 3 記録再生回路, 4 暗

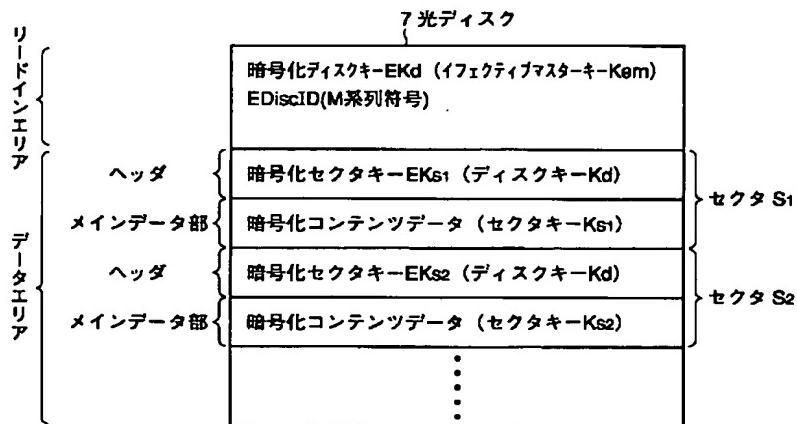
号化部, 5 復号部, 6 ピックアップ, 7 光ディスク, 8 サーボ回路, 9 スピンドルモータ, 10 乱数発生回路, 21 DiscID暗号化復号回路, 22 M系列符号発生回路, 23 Kem発生モジュール, 24 Kmメモリ, 25 hash関数回路, 26 Kd暗号化復号回

路, 27 Ks暗号化回路, 28 コンテンツデータ暗号化回路, 51 EDiscID復号回路, 52 M系列符号発生回路, 53 Kem発生モジュール, 54 Kmメモリ, 55 hash関数回路, 56 EKd復号回路, 57 EKs復号回路, 58 コンテンツデータ復号回路

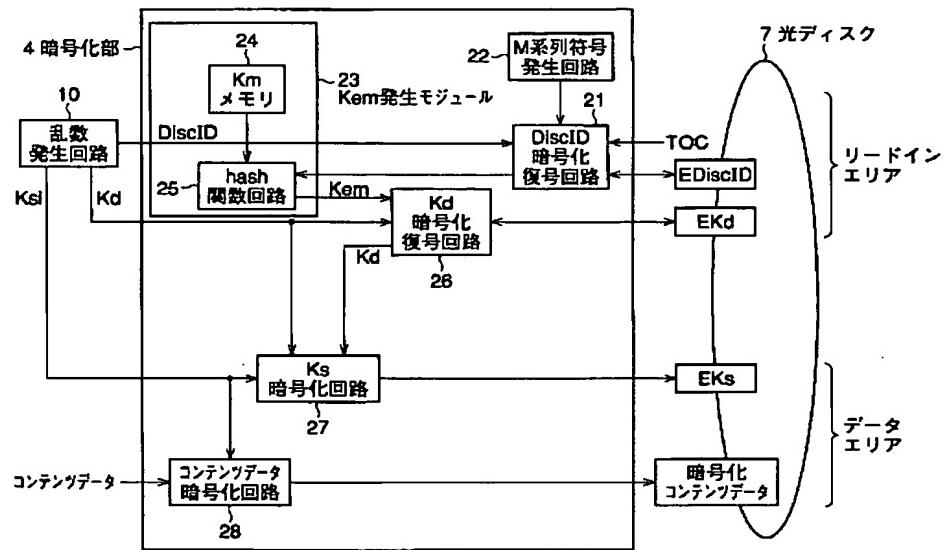
【図1】

光ディスク記録再生装置

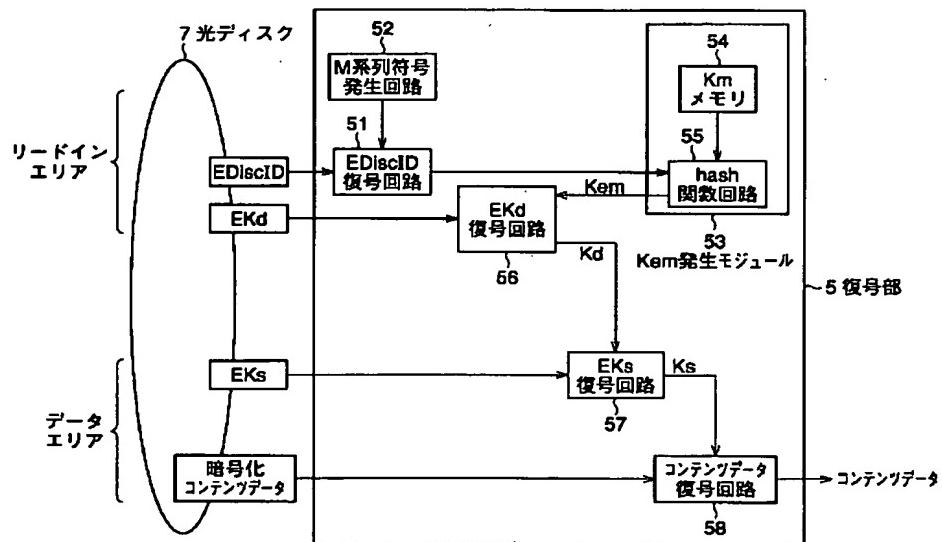
【図2】



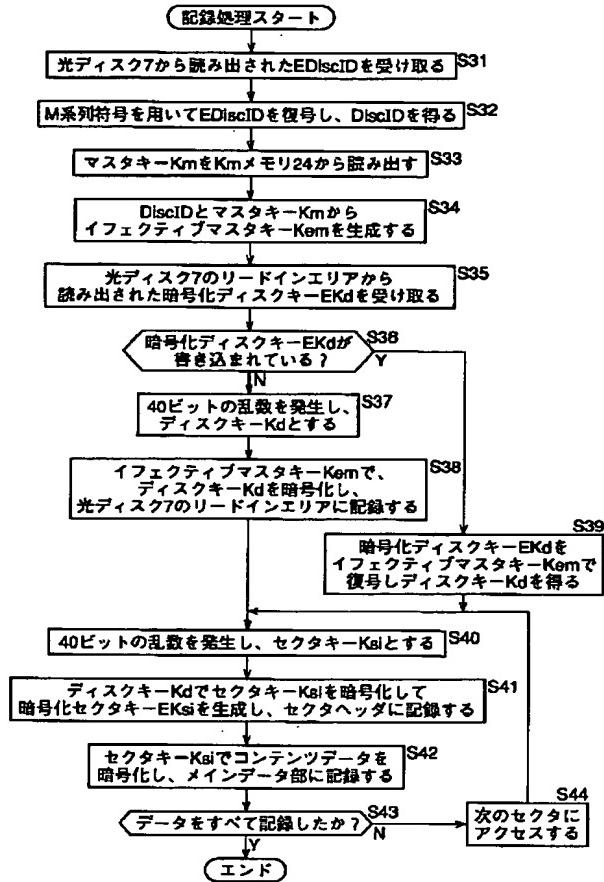
【図3】



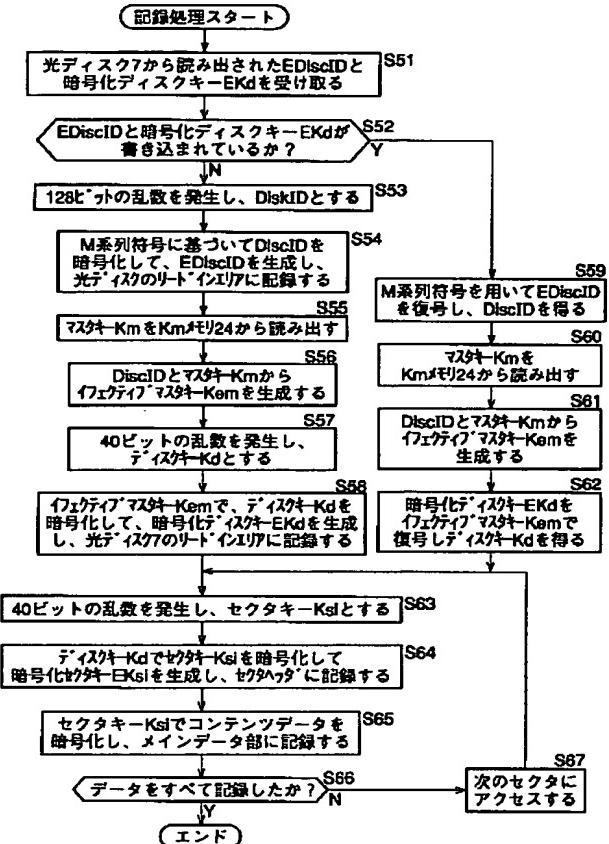
【図4】



【図5】



【図6】



【図7】

